**At least one network layout schematic indicating the security zones, their network IP addresses as well as any firewall and IDS sensor placements**

To create a network layout for the e-commerce company, we need to identify the network security zones and their requirements. Then, we'll determine appropriate IP addresses for each zone and specify firewall rules and IDS sensor placements.

Here is a high-level summary of the network security zones and their requirements:

1. DMZ (Demilitarized Zone) - Contains web servers, accessible from the internet
2. Protected Network - Contains database servers, application and financial processing servers, and internal user machines
3. Public Network - Contains external users, which need access to the web servers

Let's assume the assigned Class C network address is 192.168.0.0 with a 24-bit subnet mask (255.255.255.0). We'll subnet this network into smaller networks to create the required security zones.

Subnetting:

1. DMZ: 192.168.0.0/26 (255.255.255.192) - 62 hosts
2. Protected Network: 192.168.0.64/26 (255.255.255.192) - 62 hosts
3. Public Network: 192.168.0.128/25 (255.255.255.128) - 126 hosts

Now we can assign IP addresses to the various servers and devices in the security zones:

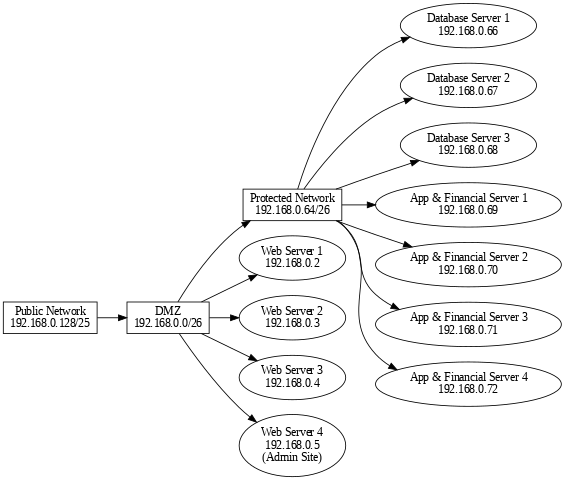
1. DMZ:
   * Web Server 1: 192.168.0.2
   * Web Server 2: 192.168.0.3
   * Web Server 3: 192.168.0.4
   * Web Server 4: 192.168.0.5 (Admin site at "/var/www/admin/admin.htm")
2. Protected Network:
   * Database Server 1: 192.168.0.66
   * Database Server 2: 192.168.0.67
   * Database Server 3: 192.168.0.68
   * App & Financial Server 1: 192.168.0.69
   * App & Financial Server 2: 192.168.0.70
   * App & Financial Server 3: 192.168.0.71
   * App & Financial Server 4: 192.168.0.72
   * Database Administrator: 192.168.0.73
   * Internal Users (Multiple): 192.168.0.74 - 192.168.0.126

Firewall Rules:

1. Allow incoming HTTP (80) and HTTPS (443) traffic from the Public Network to the DMZ.
2. Allow incoming SSH (22) traffic from the Protected Network to the DMZ and application servers.
3. Allow the Database Administrator to access the database servers on port 3306.
4. Allow the web servers to communicate with the database servers on the custom port 3245.
5. Allow the web servers to communicate with the financial processing servers on the custom port 3272.
6. Restrict remote access to the administration site on Web Server 4 to only hosts located in the Protected Network subnet (192.168.0.64/26).

IDS Placement:

1. Place an IDS sensor between the DMZ and Protected Network to monitor traffic between the zones.
2. Place an IDS sensor at the ingress/egress points of the Protected Network to monitor traffic entering and leaving the network.



**A document containing the firewall pseudo-code rules necessary to enforce your design**

These rules are written in pseudo-code and can be adapted to the specific syntax of the firewall system you are using. Make sure to implement these rules in the appropriate order, as firewall rules are processed in a top-down manner. The first rule that matches a packet determines the action taken (e.g., ALLOW or DENY).

# Allow incoming HTTP and HTTPS traffic from the Public Network to the DMZ

Rule 1:

    Source IP: 192.168.0.128/25 (Public Network)

    Destination IP: 192.168.0.0/26 (DMZ)

    Protocol: TCP

    Destination Port: 80 (HTTP) or 443 (HTTPS)

    Action: ALLOW

# Allow incoming SSH traffic from the Protected Network to the DMZ and application servers

Rule 2:

    Source IP: 192.168.0.64/26 (Protected Network)

    Destination IP: 192.168.0.0/26 (DMZ) and 192.168.0.69-192.168.0.72 (App & Financial Servers)

    Protocol: TCP

    Destination Port: 22 (SSH)

    Action: ALLOW

# Allow the Database Administrator to access the database servers on port 3306

Rule 3:

    Source IP: 192.168.0.73 (Database Administrator)

    Destination IP: 192.168.0.66-192.168.0.68 (Database Servers)

    Protocol: TCP

    Destination Port: 3306

    Action: ALLOW

# Allow the web servers to communicate with the database servers on custom port 3245

Rule 4:

    Source IP: 192.168.0.2-192.168.0.5 (Web Servers)

    Destination IP: 192.168.0.66-192.168.0.68 (Database Servers)

    Protocol: TCP

    Destination Port: 3245

    Action: ALLOW

# Allow the web servers to communicate with the financial processing servers on custom port 3272

Rule 5:

    Source IP: 192.168.0.2-192.168.0.5 (Web Servers)

    Destination IP: 192.168.0.69-192.168.0.72 (App & Financial Servers)

    Protocol: TCP

    Destination Port: 3272

    Action: ALLOW

# Restrict remote access to the administration site on Web Server 4 to only hosts located in the Protected Network subnet

Rule 6:

    Source IP: 192.168.0.64/26 (Protected Network)

    Destination IP: 192.168.0.5 (Web Server 4 - Admin site)

    Protocol: TCP

    Destination Port: 443 (HTTPS)

    Action: ALLOW

# Deny any other traffic that does not match the rules above

Rule 7:

    Action: DENY

**A document containing any Apache directives necessary to implement the administration website**

# Load necessary Apache modules

LoadModule ssl\_module modules/mod\_ssl.so

LoadModule authz\_core\_module modules/mod\_authz\_core.so

LoadModule authz\_host\_module modules/mod\_authz\_host.so

# Define the main server configuration

<VirtualHost \*:80>

    ServerName www.example.com

    DocumentRoot /var/www/html

    # Redirect all HTTP traffic to HTTPS for security

    Redirect permanent / https://www.example.com/

</VirtualHost>

# Define the HTTPS server configuration

<VirtualHost \*:443>

    ServerName www.example.com

    DocumentRoot /var/www/html

    # Enable SSL

    SSLEngine on

    SSLCertificateFile /path/to/your/certificate.crt

    SSLCertificateKeyFile /path/to/your/privatekey.key

    SSLCertificateChainFile /path/to/your/chain.crt

    # Define the administration website configuration

    <Directory "/var/www/html/admin">

        # Allow access from the Protected Network subnet only

        Require ip 192.168.0.64/26

        # Set up password authentication

        AuthType Basic

        AuthName "Restricted Content"

        AuthUserFile /etc/apache2/.htpasswd

        Require valid-user

    </Directory>

    # Define a separate alias for the administration website

    Alias "/admin" "/var/www/html/admin/admin.htm"

    # Configure logging

    LogLevel warn

    ErrorLog ${APACHE\_LOG\_DIR}/error.log

    CustomLog ${APACHE\_LOG\_DIR}/access.log combined

</VirtualHost>

In this configuration, we first ensure that the necessary Apache modules are loaded. The main server configuration listens on port 80 and redirects all traffic to the HTTPS-enabled server configuration on port 443 for improved security.

The administration website is set up within the "/var/www/html/admin" directory. We restrict access to the administration website to only the hosts in the Protected Network subnet (192.168.0.64/26) using the "Require ip" directive.

The configuration also sets up basic password authentication using an ".htpasswd" file for user validation. Make sure to create the ".htpasswd" file with the desired username and password.

Finally, an alias is created for the administration website at "/admin", which points to the "/var/www/html/admin/admin.htm" file.

Please ensure that the paths and filenames in the configuration are correct and relevant to your specific setup. You may need to replace **www.example.com** with the domain name of your e-commerce website and update the SSL certificate paths to match your server's environment.

**OPTIONAL Bonus**

I have already provided above with a subnetted Class C network address, where the given network address was 192.168.0.0 with a 24-bit subnet mask (255.255.255.0). I am going explore a different Class C network address to demonstrate the subnetting process again.

Assume that you are assigned a Class C network address of 192.168.1.0 with a 24-bit subnet mask (255.255.255.0). Our goal is to further subnet this network address to create smaller networks for the DMZ, Protected Network, and Public Network.

For this scenario, let's assume the following:

1. DMZ requires 4 web servers.
2. Protected Network requires 3 database servers, 4 application and financial processing servers, a Database Administrator, and internal users.
3. Public Network requires external users' access to the web servers.

To fulfill these requirements, we can borrow bits from the host portion of the address to create subnets.

Subnetting:

1. DMZ:
   * Required hosts: 4
   * Borrow 2 bits: 2^2 = 4 (Subnets)
   * New subnet mask: 255.255.255.192 (26 bits)
   * Usable IP addresses: 62
   * IP address range: 192.168.1.0/26
2. Protected Network:
   * Required hosts: 40 (approximately)
   * Borrow 1 bit: 2^1 = 2 (Subnets)
   * New subnet mask: 255.255.255.128 (25 bits)
   * Usable IP addresses: 126
   * IP address range: 192.168.1.64/25
3. Public Network:
   * Remaining subnet
   * Subnet mask: 255.255.255.128 (25 bits)
   * Usable IP addresses: 126
   * IP address range: 192.168.1.128/25

By borrowing bits from the host portion of the address, we have created smaller networks for the DMZ, Protected Network, and Public Network while accommodating the number of hosts required in each network. This optimizes the IP address allocation and ensures efficient network usage.

